

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-190529

(43)Date of publication of application : 23.07.1996

(51)Int.Cl.

G06F 15/00
G06F 9/445
G06F 9/06
G06F 17/60

(21)Application number : 07-001798

(71)Applicant : FUJITSU LTD

(22)Date of filing : 10.01.1995

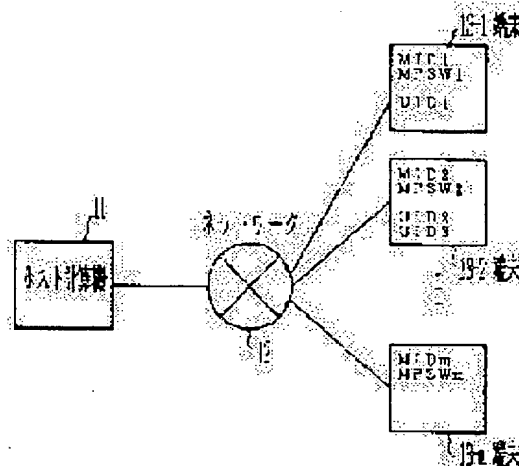
(72)Inventor : OKADA TOSHIO
IGARASHI NORIHIKO
OKI HIROSHI
KAMATA SHINJI
HARA TAKASHI
YAMAZAKI TOSHIYA

(54) IDENTIFIER MANAGEMENT DEVICE AND METHOD FOR SOFTWARE CIRCULATION SYSTEM

(57)Abstract:

PURPOSE: To manage the distribution destinations in a software circulation system based on the information including an identifier and to monitor the illegal copies.

CONSTITUTION: When a host computer 11 of a circulation center sales the software in response to the request given from a user terminal and via a network 12, a terminal identifier (MID) and a terminal password (MPSW) are given to each terminal. At the same time, a user identifier (UID) and a user password are given to the user. Furthermore, a distribution identifier is buried into the software and sold. The computer 11 secures the relation between these identifiers and passwords and manages the sales histories. If the sold software is destroyed, the restoration service is given to the software based on its sales record. And, the terminal password is rewritten every time the computer 11 receives an access and it is checked whether the latest terminal password is used for every access or not.



LEGAL STATUS

[Date of request for examination] 12.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3366143

[Date of registration] 01.11.2002

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11) 特許出願公開番号

特開平8-190529

(43) 公開日 平成 8 年 (1996) 7 月 23 日

(51) Int.Cl. ⁴	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 9 0	9364-5L		
9/445				
9/06	5 5 0 G			

G 0 6 F 9/ 06 4 2 0 J
15/ 21 Z

審査請求 未請求 請求項の数24 O L (全 14 頁) 最終頁に続く

(21) 出願番号 特願平7-1798

(22) 出願日 平成 7 年 (1995) 1 月 10 日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 岡田 利司郎

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72) 発明者 五十嵐 典彦

神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74) 代理人 弁理士 大曾 義之 (外 1 名)

最終頁に続く

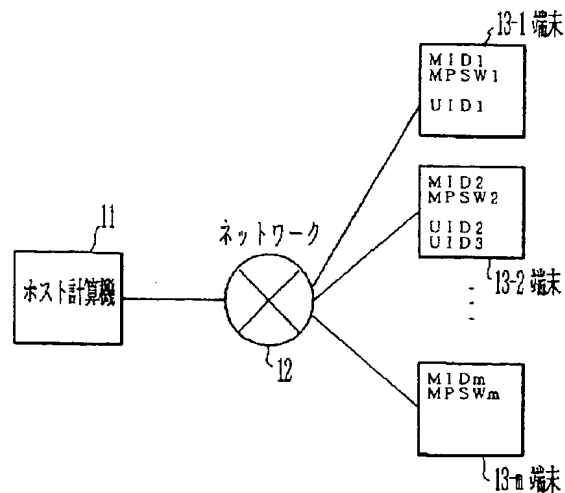
(54) 【発明の名称】 ソフトウェア流通システムにおける識別子管理装置および方法

(57) 【要約】 (修正有)

【目的】 流通ソフトウェアの配布先を識別子を含む情報によって管理し、不正コピーを監視する。

【構成】 流通センターのホスト計算機 11 がユーザの端末からの要請に応じて、ネットワーク 12 を介してソフトウェアを販売する際、各端末には、それぞれの端末識別子 (MID) 及び端末パスワード (MPSW) が付与され、ユーザには、ユーザ識別子 (UID) 及びユーザパスワードが付与される。また、ソフトウェアには、ディストリビューション識別子が埋め込まれて販売される。ホスト計算機 11 は、これらの識別子及びパスワードを関連付けて、販売の履歴を管理する。販売したソフトウェアが破壊されたときは、その販売記録を参照して復旧サービスが行われる。また、ホスト計算機 11 にアクセスするたびに、端末の端末パスワードは書き換えられ、最新の端末パスワードを用いてアクセスしているかどうかチェックされる。

実施例の構成図



【特許請求の範囲】

【請求項 1】 流通センターとユーザの端末とをネットワークで結び、該流通センターからオンラインでソフトウェアを該端末に配布するソフトウェア流通システムにおいて、

前記ソフトウェアを格納するソフトウェア格納手段と、
前記ソフトウェアの配布先の前記ユーザの識別子を含むユーザ情報を記憶するユーザ情報記憶手段と、
前記ソフトウェアがインストールされる端末の識別子を含む端末情報を記憶する端末情報記憶手段と、
前記ユーザ情報記憶手段に記憶された前記ユーザ情報と前記端末情報記憶手段に記憶された前記端末情報とを関連付けて管理する管理手段とを備えることを特徴とする識別子管理装置。

【請求項 2】 前記ソフトウェアの配布記録を前記端末の識別子と関連付けて記憶する配布記録記憶手段をさらに備え、
前記管理手段は、前記ユーザ情報と前記端末情報と前記配布記録とを用いて、前記ソフトウェアの配布の履歴を管理することを特徴とする請求項 1 記載の識別子管理装置。

【請求項 3】 前記ユーザ情報記憶手段は、前記ユーザの名前を含む前記ユーザ情報を記憶し、
前記端末情報記憶手段は、前記ソフトウェアがインストールされる端末の機種を含む前記端末情報を記憶し、
前記配布記録記憶手段は、前記ソフトウェアの名称と配布日時を含む前記配布記録を記憶し、
前記管理手段は、前記ユーザの名前、前記端末の機種、前記ソフトウェアの名称、および前記配布日時を含む前記履歴を管理することを特徴とする請求項 2 記載の識別子管理装置。

【請求項 4】 前記ソフトウェアがインストール時以降に使用不可能となったとき、前記管理手段は前記ユーザ情報と前記端末情報と前記配布記録とを参照して、該ソフトウェアの復旧サービスを前記ユーザに提供することができることを特徴とする請求項 2 記載の識別子管理装置。

【請求項 5】 前記管理手段は、前記ソフトウェアの配布サービスの代金を前記ユーザに課金することを特徴とする請求項 2 記載の識別子管理装置。

【請求項 6】 前記配布記録記憶手段は、前記ユーザに前記ソフトウェアを販売したかどうかを示す前記配布記録を記憶し、
前記ソフトウェアがインストール時以降に使用不可能となったとき、前記管理手段は前記ユーザ情報と前記配布記録とを参照して、前記ユーザに該ソフトウェアを販売したことがわかった場合に、該ソフトウェアの復旧を行うことを特徴とする請求項 5 記載の識別子管理装置。

【請求項 7】 前記管理手段は、前記ソフトウェアの配布サービスの代金を前記端末に課金することを特徴とす

る請求項 2 記載の識別子管理装置。

【請求項 8】 前記配布記録記憶手段は、前記端末に前記ソフトウェアを販売したかどうかを示す前記配布記録を記憶し、

前記ソフトウェアがインストール時以降に使用不可能となったとき、前記管理手段は前記端末情報と前記配布記録とを参照して、前記端末に該ソフトウェアを販売したことがわかった場合に、該ソフトウェアの復旧を行うことを特徴とする請求項 7 記載の識別子管理装置。

10 【請求項 9】 前記管理手段は、前記ユーザ情報と前記端末情報と前記配布記録とを参照して、前記ユーザに前記ソフトウェアに関するサービス情報を提供することを特徴とする請求項 2 記載の識別子管理装置。

【請求項 10】 前記サービス情報は、前記ソフトウェアのバージョンアップに関する情報を含むことを特徴とする請求項 9 記載の識別子管理装置。

【請求項 11】 前記ソフトウェアがインストールされる端末が第 1 のユーザから第 2 のユーザに譲渡された場合に、前記管理手段は該第 1 のユーザの識別子の代わりに該第 2 のユーザの識別子を前記端末の識別子と関連付けることにより、該端末に付属する前記ソフトウェアに関する権利を該第 2 のユーザに移すことを特徴とする請求項 1 記載の識別子管理装置。

【請求項 12】 前記ユーザ情報記憶手段は、前記ユーザが前記ユーザの識別子に対応して設定したユーザパスワードを含む前記ユーザ情報を記憶し、
前記管理手段は、前記ユーザの識別子と前記ユーザパスワードとを用いて、ユーザからのアクセスを識別することを特徴とする請求項 1 記載の識別子管理装置。

30 【請求項 13】 前記端末情報記憶手段は、前記端末の識別子に対応して付与された第 1 の端末パスワードを含む前記端末情報を記憶し、
前記管理手段は、前記端末の識別子と前記第 1 の端末パスワードとを用いて、端末からのアクセスを識別することを特徴とする請求項 1 記載の識別子管理装置。

【請求項 14】 前記第 1 の端末パスワードを持つ端末からのアクセスがあったとき、該第 1 の端末パスワードを第 2 の端末パスワードに変更する端末パスワード変更手段をさらに備え、

40 前記管理手段は、該第 2 の端末パスワードを前記端末の識別子に対応させることを特徴とする請求項 13 記載の識別子管理装置。

【請求項 15】 前記端末の識別子を持ち、該端末の識別子に対応していない端末パスワードを持つ端末からのアクセスがあったとき、前記管理手段は該対応していない端末パスワードを持つ端末に新しい識別子を付与して、新規に管理することを特徴とする請求項 14 記載の識別子管理装置。

50 【請求項 16】 流通センターとユーザの端末とをネットワークで結び、該流通センターからオンラインでソフ

トウェアを該端末に配布するソフトウェア流通システムにおいて、

前記ソフトウェアを格納するソフトウェア格納手段と、前記ソフトウェア格納手段に格納された前記ソフトウェア内にディストリビューション識別子を書き込むディストリビューション識別子付加手段とを備えることを特徴とする識別子管理装置。

【請求項 17】 前記ディストリビューション識別子の書き込みのための情報を記述した定義ファイルを格納する定義ファイル格納手段をさらに備え、

前記ディストリビューション識別子付加手段は、前記ソフトウェアを配布するときに前記定義ファイル格納手段に格納された前記定義ファイルを参照して、前記ソフトウェア内に前記ディストリビューション識別子を書き込むことを特徴とする請求項 16 記載の識別子管理装置。

【請求項 18】 前記書き込みのための情報は、前記ソフトウェア内に設けられた、前記ディストリビューション識別子の書き込み領域の位置を含むことを特徴とする請求項 17 記載の識別子管理装置。

【請求項 19】 前記定義ファイルを参照して、前記流通センターにアクセスするユーザが持っている前記ソフトウェアの前記ディストリビューション識別子をチェックする管理手段をさらに備えることを特徴とする請求項 17 記載の識別子管理装置。

【請求項 20】 前記ソフトウェアの配布記録を記憶する配布記録記憶手段をさらに備え、

前記ディストリビューション識別子付加手段は、前記ソフトウェアを配布するときに前記配布記録記憶手段に記憶された前記配布記録に前記ディストリビューション識別子を書き込むことを特徴とする請求項 16 記載の識別子管理装置。

【請求項 21】 流通センターとユーザの端末とをネットワークで結び、該流通センターからオンラインでソフトウェアを該端末に配布する方法において、前記ソフトウェアの配布先の前記ユーザの識別子を含むユーザ情報を保持し、

前記ソフトウェアがインストールされる端末の識別子を含む端末情報を保持し、

前記ユーザ情報と前記端末情報とを関連付けて管理することを特徴とする識別子管理方法。

【請求項 22】 前記ソフトウェアの配布記録を前記端末の識別子と関連付けて保持し、前記ユーザ情報と前記端末情報と前記配布記録とを用いて、前記ソフトウェアの配布の履歴を管理することを特徴とする請求項 21 記載の識別子管理方法。

【請求項 23】 前記端末の識別子に対応して第 1 の端末パスワードを付与し、

前記端末の識別子と前記第 1 の端末パスワードとを用いて、前記端末からのアクセスを識別し、

前記第 1 の端末パスワードを持つ端末からのアクセスが

あったとき、該第 1 の端末パスワードを第 2 の端末パスワードに変更して、該第 2 の端末パスワードを前記端末の識別子に対応させることを特徴とする請求項 21 記載の識別子管理装置。

【請求項 24】 流通センターとユーザの端末とをネットワークで結び、該流通センターからオンラインでソフトウェアを該端末に配布する方法において、

前記ソフトウェア内にディストリビューション識別子を書き込み、

10 前記ディストリビューション識別子を用いて、配布した前記ソフトウェアを識別することを特徴とする識別子管理方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はネットワークを介したソフトウェアの流通（ディストリビューション）システムに係り、ソフトウェアの配布先の識別子を管理する装置とその方法に関する。

【0002】

20 【従来技術】現在、店頭で販売されているパッケージソフトウェアは、一般に、インストールするパソコン等のマシンの台数や同時に動作可能なマシンの台数に制限を設けていることが多い。例えば、1 台のパソコンのみにインストール可能であるとか、または複数のパソコンにインストール可能だが、そのうち同時に動作してもよい台数は 1 台のみであるというような制限である。

【0003】例えば、WINDOWS 上に搭載されるソフトウェア等においてはその不正コピーを抑制するため、インストール時にライセンス登録情報をフロッピーディスク上のソフトウェアに書き込むことが一般的になってきている。しかし、このライセンス登録情報はときとして偽りの情報であったり、フリーウェア等で後から自由に書き直したりすることが可能であったりするため、十分な効果が得られていない。

【0004】一方、近年のパソコン通信等の発達に伴い、ネットワークを介してオンラインでソフトウェアを購入できることが望まれている。このようなソフトウェアの流通を実現するにあたって、ベンダーとユーザの間におけるソフトウェアの使用契約等のいくつかの問題がある。例えば、上述したようなソフトウェアのインストール時および使用時における制限を設け、それを実施するためには、ソフトウェアの使用状況を管理する工夫が必要になる。

【0005】

【発明が解決しようとする課題】ネットワークを介したオンラインのソフトウェア流通システムを構築するには次のような問題がある。

【0006】フロッピーディスクを利用した現在のプロテクション方法は用いることができず、インストールしたマシンから別のマシンへソフトウェアが不正にコピー

される恐れがあり、このような不正コピーを監視する機構が必要になる。

【0007】また、何らかの原因によりインストールしたソフトウェアが破壊されて使用不可能となったときに、ユーザの復旧要請に応じる必要がある。また、将来、オンラインによるソフトウェアの流通が一般に普及した場合に、配布したソフトウェアを個別に識別する機構が必要になる。

【0008】本発明は、ネットワークを介したソフトウェアの流通システムにおいて、ソフトウェアの配布先の識別子を含む情報を管理し、ベンダーまたはユーザの利益を図る識別子管理装置とその方法を提供することを目的とする。

【0009】

【課題を解決するための手段】本発明は、流通センターとユーザの端末とをネットワークで結び、流通センターからオンラインでソフトウェアを端末に配布するソフトウェア流通システムにおける識別子管理装置および識別子管理方法である。

【0010】図1は、本発明の識別子管理装置の原理図である。図1の識別子管理装置は、管理手段1、端末パスワード変更手段2、ディストリビューション識別子付加手段3、ユーザ情報記憶手段4、端末情報記憶手段5、配布記録記憶手段6、定義ファイル格納手段7、およびソフトウェア格納手段8を備える。

【0011】ソフトウェア格納手段8は配布するソフトウェアを格納し、ユーザ情報記憶手段4はソフトウェアの配布先のユーザの識別子を含むユーザ情報を記憶し、端末情報記憶手段5はソフトウェアがインストールされる端末の識別子を含む端末情報を記憶する。管理手段1は、ユーザ情報記憶手段4に記憶された上記ユーザ情報と端末情報記憶手段5に記憶された上記端末情報とを関連付けて管理する。

【0012】配布記録記憶手段6はソフトウェアの配布記録を上記端末の識別子と関連付けて記憶し、管理手段1は前記ユーザ情報と上記端末情報と上記配布記録とを用いて、ソフトウェアの配布の履歴を管理する。

【0013】また、端末情報記憶手段5は上記端末の識別子に対応して付与された第1の端末パスワードを含む上記端末情報を記憶し、管理手段1は上記端末の識別子と上記第1の端末パスワードとを用いて端末からのアクセスを識別する。

【0014】端末パスワード変更手段2は上記第1の端末パスワードを持つ端末からのアクセスがあったとき、第1の端末パスワードを第2の端末パスワードに変更し、管理手段1は第2の端末パスワードを上記端末の識別子に対応させる。

【0015】定義ファイル格納手段7はディストリビューション識別子の書き込みのための情報を記述した定義ファイルを格納する。ソフトウェアを配布するときに、

ディストリビューション識別子付加手段3は定義ファイル格納手段7に格納された上記定義ファイルを参照して、ソフトウェア格納手段8に格納されたソフトウェア内に上記ディストリビューション識別子を書き込むとともに、配布記録記憶手段6に記憶された上記配布記録に上記ディストリビューション識別子を書き込む。

【0016】また、管理手段1は上記定義ファイルを参照して、上記流通センターにアクセスするユーザが持っているソフトウェアの上記ディストリビューション識別子をチェックする。

【0017】図1の管理手段1、端末パスワード変更手段2、およびディストリビューション識別子付加手段3は、図2に示す実施例におけるホスト計算機11内の図示されない処理装置に相当する。また、図1のユーザ情報記憶手段4、端末情報記憶手段5、配布記録記憶手段6、定義ファイル格納手段7、およびソフトウェア格納手段8は、図2のホスト計算機11内の図示されない記憶装置に相当する。

【0018】また、上記配布記録は例えば図4、5、および13に示す販売記録に相当し、上記定義ファイルに記述された上記書き込みのための情報とは、例えば上記ディストリビューション識別子を書き込むファイルの名称、そのファイル内の書き込み領域の位置、その書き込み領域の大きさ等の情報である。

【0019】

【作用】管理手段1によりユーザ情報記憶手段4の記憶するユーザの識別子と端末情報記憶手段5の記憶する端末の識別子とが関連付けて管理される。これにより、ソフトウェアがどのユーザに対して配布され、またその際の端末にインストールされたかが同時に把握される。

【0020】さらに、配布記録記憶手段6が記憶する配布記録が上記端末の識別子と関連付けられるので、一つのソフトウェアの配布の履歴がインストールした端末の端末情報とともに管理される。

【0021】また、端末情報記憶手段5内の端末情報と端末内の双方に、上記端末の識別子に対応した第1の端末パスワードが保持される。端末からのアクセスがあったとき、管理手段1は上記端末の識別子と第1の端末パスワードとを用いて、アクセスした端末を識別する。例えば、アクセスした端末の持つ端末パスワードがその端末の識別子に対応していない場合は、その端末側に何かの異変があったとみなすことができる。

【0022】さらに、端末からのアクセスがあったとき、端末パスワード変更手段2によりその端末の第1の端末パスワードが第2の端末パスワードに変更される。これにより、次のアクセス時には、上記端末の識別子と第2の端末パスワードとを用いて端末の識別が行われる。もし、ユーザが端末にインストールされたソフトウェアを上記端末の識別子と第1の端末パスワードとともに別の端末にコピーして、次のアクセス時に別の端末

からアクセスしても、既に第 1 の端末パスワードは有効性を失っているため管理手段 1 は異常を察知することができる。

【0023】また、定義ファイル格納手段 7 内の定義ファイルに記述された書き込みのための情報に従って、ディストリビューション識別子付加手段 3 により、配布するソフトウェア内にディストリビューション識別子が書き込まれる。管理手段 1 は上記定義ファイルを参照して、ユーザの持つソフトウェアの上記ディストリビューション識別子をチェックすることができる。例えば、上記ディストリビューション識別子として配布先のユーザの識別子を用いれば、アクセスしてきたユーザが配布時のユーザと同一かどうか分かる。

【0024】配布記録記憶手段 6 内の上記配布記録にも上記ディストリビューション識別子を書き込んでおくことにより、管理手段 1 は上記配布記録内のディストリビューション識別子とユーザの持つソフトウェア内に書き込まれたものとを比較できる。

【0025】

【実施例】以下、図面を参照しながら、本発明の実施例について詳細に説明する。図 2 は、本発明の一実施例のソフトウェア流通システムの構成図である。図 2 のソフトウェア流通システムは、ホスト計算機 11 と複数 (m 個) のユーザ端末 13-1、・・・、13-m、およびそれらを結合するネットワーク 12 から成る。

【0026】ホスト計算機 11 はソフトウェアの流通センターにあり、端末 13-1、・・・、13-m からの要請に応じて、ネットワーク 12 を介してソフトウェアを販売する。端末 13-1、・・・、13-m は例えばユーザの自宅やオフィス等に設置されたパソコン等の計算機であり、ネットワーク 12 を介して希望するソフトウェアを購入し、購入したソフトウェアを使用してホスト計算機 11 にアクセスする。

【0027】ホスト計算機 11 は本発明の識別子管理装置を含み、販売するソフトウェアを格納するための図示されない記憶装置を有する。ホスト計算機 11 は端末 13-1、・・・、13-m にそれぞれの端末識別子 (マシン ID) MID1、・・・、MIDm を発行し、端末のユーザにはマシン ID とは別のユーザ識別子 (ユーザ ID) UID1、UID2、UID3 等を発行する。また、各マシン ID に対応して端末のパスワード (マシンパスワード) MP SW1、・・・、MP SWm を設け、各ユーザ ID に対応してユーザパスワード (不図示) を設ける。ホスト計算機 11 はこれらのマシン ID、マシンパスワード、ユーザ ID、およびユーザパスワードを用いて、ソフトウェアの販売先である端末とユーザの情報を管理する。

【0028】ユーザに販売したソフトウェアが何らかの原因により破壊され使用不可能となった場合には、ホスト計算機 11 は販売記録を参照して、そのソフトウェア

の復旧サービスを行う。また、販売したソフトウェアのバージョンアップのサービスも行う。さらに、ホスト計算機 11 は端末に与えるマシンパスワードを動的に変更して、アクセスが行われるたびにそれをチェックすることにより、インストールしたソフトウェアが他の端末にコピーされたかどうかを監視する。

【0029】あるユーザから他のユーザに端末の譲渡があった場合には、その端末にインストールされたソフトウェアは、そのバージョンアップや復旧等のサービスを受ける権利も含めて譲り渡すことが可能となる。このような譲渡を行えば、不正コピーの防止にも繋がるし、権利の譲渡もスムーズに行われるため、ユーザとベンダーの双方に有益に働く。

【0030】図 3 および図 4 は、それぞれホスト計算機 11 内の記憶領域に格納されるユーザ情報および端末情報 (マシン情報) の例を示している。図 3 のユーザ情報は、ユーザ ID (UID)、ユーザパスワード (PSW)、マシン ID (MID)、ユーザの名前等から成り、図 4 のマシン情報は、MID、マシンパスワード (MP SW)、UID、端末の機種、ソフトウェアの販売記録等から成る。

【0031】図 5 は、図 4 のソフトウェアの販売記録の例を示している。図 5 の販売記録は、販売したソフトウェアの名称 (ソフトウェア名)、購入したユーザの UID、販売日時から成る。

【0032】このように、ホスト計算機 11 は MID、UID、およびソフトウェアの販売記録を互いに関連付けて記憶し、ソフトウェアの販売先の情報として管理する。これにより、いつ、誰が、どの端末に、どんなソフトウェアをインストールしたかを示す販売履歴の管理が可能となる。また、そのソフトウェアに関するバージョンアップ等のサービス情報を購入したユーザのみに選択的に提供して、購入者を優遇することもできる。

【0033】ところで、個人や企業がパソコン等の端末を持つ場合、ソフトウェアの購入のために代金を支払う人と購入したソフトウェアを使用する人の関係、あるいはソフトウェアを購入または使用する人と端末との関係が必ずしも 1 対 1 の関係では無く、次のような形態が生じ得る。

- (1) 1 人のユーザが複数台の端末を持つ。
- (2) 複数のユーザが 1 台の端末を共有する。
- (3) (1) と (2) の混合形態。

【0034】これらの各形態に対応するソフトウェアの使用契約としては、次のような形態が考えられる。

(1) 1 台の端末にのみソフトウェアのインストールが許される。

(2) 複数の端末にソフトウェアをインストールしてもよいが、そのソフトウェアを 2 つ以上の端末上で同時に使用することは禁止される。

(3) 複数の端末にソフトウェアをインストールして、

それらの端末上で同時に使用してもよい（フリーウェア）。

【0035】また、これらの各契約形態に対応する管理方法は次のようになる。

- (1) ソフトウェアをどの端末にインストールしたかを、MIDと関連させて管理する必要がある。
- (2) ソフトウェアをどのユーザに販売したかを、UIDと関連させて管理する必要がある。
- (3) フリーウェア等に相当し、販売先の管理は不要である。

【0036】上記(1)および(2)の使用形態を管理するには、MIDとUIDの両方を用いる必要がある。本実施例では、流通センターのホスト計算機11が契約したすべてのユーザにユニークなUIDを与え、また契約したすべての端末にユニークなMIDを与える。

【0037】ホスト計算機11は商品（ソフトウェア）の販売時に、UIDを用いて代金を支払うべきユーザを特定する。したがって、あるUIDを用いて販売されたソフトウェアの代金は、そのUIDを持つユーザが支払う契約になっている。また、販売された商品はその販売先の端末のMIDと関連付けられて管理される。これにより、ある商品を誰が購入し、どの端末にインストールされたかが明確になり、その商品が破壊された場合でも無償の復旧サービス等を提供することが可能になる。

【0038】図6は、1人のユーザが複数の端末を持つ場合に、ホスト計算機11が管理する情報の関係を示している。図6において、ユーザ情報は、UID=01、ユーザの氏名、キャッシュカードの情報（キャッシュカードの番号等）、およびソフトウェアの購入情報から成る。購入情報は過去にそのユーザが流通センターから購入したソフトウェア名と購入金額のリストであり、例えばそのユーザのUIDを持つ販売記録を参照して得ることができる。ここでは、UID=01を持つユーザがLOTUS-WIN、FM秘書、LOTUS、OASYSの各ソフトウェアを購入したことがわかる。

【0039】UID=01のユーザが持つ3つの端末PC98、TOWNS、およびFMRのうち、MID=11のPC98とMID=10のTOWNSとがホスト計算機11に登録されており、その登録時にUID=01と関係付けられる。登録時には、図4に示すように端末のマシン情報にUIDを書き込んでもよく、あるいはまた、ポインタ等を用いてマシン情報とユーザ情報を結びつけてもよい。

【0040】登録された端末のマシン情報は、MID、過去に販売されてその端末にインストールされたソフトウェアの情報（ソフト情報）、および端末の機種や使用OS（オペレーティングシステム）の情報から成る。ソフト情報は図4の販売記録に相当する。ここでは、MID=11の端末にインストールされたソフトウェアがLOTUSであり、その機種（M）は98、使用OSはD

OSであることがわかる。また、MID=10の端末にインストールされたソフトウェアはLOTUS-WINであり、その機種はTOWNS、使用OSはDOS、TOS（TOWNS用のOS）、およびWIN（WINDOWS）であることがわかる。尚、FMRにはOASYSがインストールされているが、ホスト計算機11に登録されていないためMIDは与えられていない。

【0041】図7は、複数のユーザが1台の端末を共有する場合に、ホスト計算機11が管理する情報の関係を示している。図7においては、ユーザC、D、Eの3人が1台の端末TOWNSを共有している。

【0042】ユーザCのユーザ情報は、UID=03、氏名C、キャッシュカードの情報、およびLOTUS-WINの購入情報から成る。また、ユーザDのユーザ情報は、UID=04、氏名D、キャッシュカードの情報、およびFM秘書の購入情報から成る。また、ユーザEのユーザ情報は、UID=05、氏名E、キャッシュカードの情報、およびLOTUSの購入情報から成る。

【0043】端末TOWNSのマシン情報は、MID=30、ソフト情報、機種M=TOWNS、およびOS=DOS/TOS/WINから成る。ここで、ソフト情報は3人の共有者に販売したすべてのソフトウェアの名称、LOTUS-WIN、FM秘書、LOTUSを含んでいる。

【0044】端末TOWNSのMIDは、端末の登録時に共有者のうちの1人の代表者のUIDと関係付けられる。ここでは、MID=30がユーザCのUIDと関係付けられている。この場合、ユーザCはMID=30の端末の問い合わせ先として3人の共有者を代表している。この例ではユーザDがFM秘書を購入しているが、FM秘書が破壊されたとき、ユーザD以外のどのユーザでもMID=30を用いて復旧の要求を行い、無料で再インストール（復旧）のサービスを受けることができる。

【0045】次に図8から図11までを参照しながら、本実施例のソフトウェア流通システムにおける処理のフローを説明する。図8は、ユーザIDの登録処理のフローチャートである。図8において処理が開始されると、まずユーザは端末を流通センターのホスト計算機11に接続して（ステップS1）、名前、キャッシュカードの番号、住所等の個人情報を入力する（ステップS2）。これを受けて、ホスト計算機11は仮のユーザIDと仮のユーザパスワードを発行して、ユーザの仮登録を行う（ステップS3）。ここで、ユーザは一旦ホスト計算機11との接続を断ち、キャッシュカードが認証されるのを待つ（ステップS4）。

【0046】キャッシュカードが認証され、流通センターから正式のユーザIDと正式のユーザパスワードとが郵送されてくると（ステップS5）、ユーザは再び端末をホスト計算機11に接続して（ステップS6）、受け

取った正式のユーザIDと正式のユーザパスワードとを入力する(ステップS7)。これにより、ホスト計算機11は正式のユーザIDとユーザパスワードを記載した郵便がユーザ本人に届いたことを確認し、そのユーザを正式に登録(本登録)して処理を終了する。このとき、郵送されたユーザパスワードと共に、別のパスワードをユーザが入力して登録することもできる。

【0047】図9は、端末IDの登録処理のフローチャートである。図9において処理が開始されると、まずユーザは端末を流通センターのホスト計算機11に接続して(ステップS11)、登録されているユーザIDとユーザパスワードを入力する(ステップS12)。その後、端末がその機種や使用OS等のマシン情報を自動的にホスト計算機11に送る(ステップS13)。ホスト計算機11は送られたマシン情報に端末IDと端末パスワードを付加して所定の形式で記憶し、それらの端末IDと端末パスワードを端末に送る(ステップS14)。こうして、発行された端末IDと端末パスワードは端末内にも保持される。

【0048】図10は、流通センターに登録されたユーザにネットワーク12を介してソフトウェアを販売する処理のフローチャートである。図10において、ユーザのリクエスト等により処理が開始されると、まずユーザの端末がネットワーク12に接続される(ステップS21)。次に、ホスト計算機11はユーザが入力したユーザIDとユーザパスワードをチェックし(ステップS22)、それらが正しくなければ(NG)、処理を終了する。

【0049】ユーザIDとユーザパスワードが正しければ(OK)、次にホスト計算機11は端末内に保持された端末IDと端末パスワードとを自動的に読み取り、これらをチェックする(ステップS23)。端末IDと端末パスワードが正しくなければ(NG)、不正コピーが行われた可能性があるので不正に対応する処理(不正処理)を行う(ステップS24)。

【0050】端末IDと端末パスワードが正しければ(OK)、商品であるソフトウェアのリストを端末の画面に表示させ、ユーザに購入する商品の選択を行わせる(ステップS25)。ユーザは表示されたリストから商品を選択し、復旧サービスの要請の場合はその旨を入力する。

【0051】次に、ホスト計算機11はユーザからの要求が新規商品の購入か既に販売した商品の復旧要請かを判断し(ステップS26)、復旧要請の場合はそのユーザの購入情報を参照して、該当する商品を過去に購入しているかどうかを調べる(ステップS27)。ユーザが購入していない商品の復旧を要請している場合は(ステップS27、NO)、復旧サービスの対象とならないので再びステップS25の処理に戻る。

【0052】ユーザが過去に購入した商品の復旧を要請

している場合は(ステップS27、YES)、ホスト計算機11はネットワーク12を介してその商品を端末に宅配し、再インストールする(ステップS29)。そして、使用契約等に基づいてユーザに課金して(ステップS30)、処理を終了する。ただし、無償で復旧サービスを行う契約が結ばれている場合は課金は行わない。

【0053】ステップS26でユーザが新規商品の購入を要求している場合は、選択された商品の販売を決定し(ステップS28)、ネットワーク12を介してその商品を端末に宅配してインストールする(ステップS29)。そして、商品の代金をユーザに課金して(ステップS30)、処理を終了する。

【0054】ステップS30においては、入力されたユーザIDを持つユーザに対して代金が課されるが、ユーザIDの管理はユーザに委ねられる。各ユーザはそのユーザパスワードを指定してユーザIDを管理する。

【0055】商品の販売契約がユーザを対象とせずに、インストールする端末に対して販売することになっている場合は、ステップS30において端末に対して代金が課金される。この場合は、ステップS27においてその端末が該当する商品を過去に購入しているかどうかを調べ、購入していたときにのみ復旧サービスを行う。

【0056】また、端末IDについては、ホスト計算機11が端末パスワードを付加し、端末が1回接続される毎にその端末の端末パスワードを自動的に書き換えて管理する。不正コピーが行われると、書き換え前の端末パスワードと共にアクセスが行われるため、その事実を認識することが可能になる。端末IDおよび端末パスワードについては、ホスト計算機11がバックトレースを行うことができる。

【0057】図11は、ステップS23における端末パスワードのチェックと書き換え、およびステップS24の不正処理のフローチャートである。図11において処理が開始されると、ホスト計算機11は接続された端末の端末パスワードを、その端末の前回接続時に付与した端末パスワードと比較する(ステップS31)。

【0058】それらが一致すれば、新しい端末パスワードを生成してその端末内に書き込み、ホスト計算機11内にも保持しておく(ステップS32)。このとき、ホスト計算機11は例えば乱数のように予想できないものを用いて、次の端末パスワードを決定する。また、書き換えられた古い端末パスワードは後で参照するために保存しておき(ステップS33)、処理を終了する。

【0059】ステップS31で2つの端末パスワードが一致しないときは、ホスト計算機11は不正コピーが行われたと判断し、接続された端末に新しい端末IDを付与して新規に管理する(ステップS34)。そして、接続時における端末パスワードを保存されている古い端末パスワードと順次比較して、その端末パスワードによるアクセスがあった日時を求める(ステップS35)。こ

れにより、不正コピーが行われたタイミングを特定して処理を終了する。

【0060】図12は、不正コピーが行われた場合の端末パスワードチェックの例を示している。図12において、端末PC Aのユーザがホスト計算機11へのN回目のアクセスの後、使用しているソフトウェアと共にMID=11とMPSW=111を、端末PC Aのハードディスク(HD)から端末PC Bのハードディスクに不正にコピーしたとする。このとき、PC A、PC B、ホスト計算機11が保持するすべてのMIDとMPSWが一致している。

【0061】次に、N+1回目のアクセスにおいてPC Aがアクセスを行う。ここでは、アクセスしたPC AのMIDとMPSWは、ホスト計算機11が記憶しているPC AのMIDとMPSWと同じなので(ステップS31)、不正コピーの事実は認識されない。そこで、ホスト計算機11はPC AのMPSWを222に書き換え、この新しいMPSWを保持する(ステップS32)。

【0062】次に、N+2回目のアクセスにおいてPC Bがアクセスを行う。このとき、アクセスしたPC BのMIDはホスト計算機11が記憶しているPC AのMIDと同じであるが、PC BのMPSWはホスト計算機11が記憶しているPC AのMPSWと一致しない(ステップS31)。ここで、PC Bが前回にアクセスしたPC Aと異なる端末であることがわかり、不正コピーがあったことが認識される。

【0063】そこで、ホスト計算機11はPC BのMIDを12に、MPSWを333に書き換え、これらのMIDとMPSWを保持する(ステップS34)。こうして、PC Bは新しい端末として登録され、新規に管理される。

【0064】このような識別子の管理を行うことにより、悪意の無い不正コピーは防ぐことが可能である。しかし、悪意があつてある程度の知識があれば、アクセス毎にMIDとMPSWを端末間でコピーして使用することも可能である。このような場合には不正コピーを検出することは困難になる。そこで、MIDやMPSWを人為的にコピーするには手間がかかるようにしておく。例えば、隠しファイルの属性を持たせる方法や、これらを分散して配置する方法、端末の個別情報の組み合わせにより暗号化しておく方法等が考えられる。

【0065】隠しファイルはMSDOS等で用いられるファイル属性の一つであり、ユーザは特別な操作をしないとその存在を知ることができないので、ここにMIDやMPSWを書き込んでおけばコピーすることが困難になる。

【0066】また、MPSWの情報を分割して、端末のハードディスクの複数の箇所に分散して書き込んでおけば、それらの情報を探すのに手間がかかり、すべての情

報が揃わなければMPSWを知ることはできない。

【0067】また、端末のシリアルナンバー、FORMATの日付、ファイルの物理位置等の機種別の情報や端末毎にバラツキのでる情報を用いて、所定の演算により正しいMPSWが得られるようにしておいてもよい。所定の演算としては、乗算、除算、EOR等の任意の演算の組合せを用いることができる。これにより、MPSWを得る手続きが複雑になる。

【0068】さらに、これらの方法を組み合わせて用いることも可能である。このようにしておけば、多大な手間をかけて多くのユーザが不正コピーを行うことは考えられなくなる。

【0069】本発明の識別子管理装置により、コンピュータに対する知識が浅いために善意ではあるが契約に違反してしまう可能性のあるユーザの権利の保護と、ベンダーの保護とが共に図られることになる。また、悪意のあるユーザに対しては、例えばソフトウェアの不正コピーを行って使用するために多大な手間が要求される。

【0070】上述した実施例によれば、ベンダーは不正コピーの事実があつたかどうかと、不正コピーが行われたタイミングを認識することができるが、どういうルートでソフトウェアがコピーされたかを知ることは必ずしも可能ではない。そこで、販売するソフトウェア自体にマークを付加して、そのマークをホスト計算機11に記憶しておく方法が考えられる。

【0071】以下、図13から図19までを参照しながら、このマークを用いた識別子管理方法について説明する。ホスト計算機11は、オンラインでソフトウェアを販売するときに、販売したソフトウェアを識別するマークとしてディストリビューションIDをそのソフトウェアに埋め込んでから送信する。このディストリビューションIDとしては、例えば販売先のユーザIDや端末ID、販売日時等の販売した事実を識別できる情報を用いる。特にディストリビューションIDとして購入したユーザのユーザIDを用いれば、ソフトウェアがコピーされた場合、それがだれに販売したものであるかを容易に知ることができる。

【0072】図13は、このときのマシン情報に含まれる販売記録の例を示している。図13の販売記録は図5の販売記録にディストリビューションID(DID)が付加された形になっている。

【0073】図14は、ディストリビューションIDの設定処理のフローチャートである。図14のディストリビューションIDの設定処理は、ソフトウェア作成者がソフトウェアを流通センターに登録するときに行われる。

【0074】図14において処理が開始されると、ホスト計算機11はまずDIDを埋め込む領域を、登録するソフトウェアのファイルの所定の位置に確保し(ステップS41)、その領域の位置を記述したインストール用

10

20

30

40

50

の定義ファイルを作成する(ステップS42)。次に、そのソフトウェアと共に定義ファイルを登録して(ステップS43)、処理を終了する。

【0075】図15は、ディストリビューションIDの埋め込み処理のフローチャートである。図15のディストリビューションIDの埋め込み処理は、図10のステップS28で販売するソフトウェアが決定した後に行われる。

【0076】図15において処理が開始されると、ホスト計算機11は販売するソフトウェアの定義ファイルを参照して、ディストリビューションIDを埋め込むファイルの名称とその中の埋め込み位置を特定する(ステップS44)。次に、そのファイルの所定の位置に所定のディストリビューションIDを書き込んで(ステップS45)、処理を終了する。

【0077】図16は、ディストリビューションIDのチェック処理のフローチャートである。図16のディストリビューションIDのチェック処理は、ユーザが特定のソフトウェアを指定して、そのソフトウェアがコピーされたものかどうかをチェックするよう要請した場合に行われる。

【0078】図16において処理が開始されると、ホスト計算機11はまず接続されたユーザの端末内に格納されているソフトウェアから、指定されたソフトウェアを検索する(ステップS51、S52)。指定されたソフトウェアがなければ処理を終了し、それがある場合は対応する定義ファイルを参照して、指定されたソフトウェアの所定の位置からディストリビューションIDを読み出す(ステップS53)。次に、販売記録を参照して、読み出したディストリビューションIDが正しいかどうかを判定する(ステップS54)。例えば、ディストリビューションIDとしてユーザIDを採用した場合は、ディストリビューションIDがアクセス時に入力されたユーザIDと一致していれば正しく、そうでなければ正しくない。

【0079】ディストリビューションIDが正しければ、そのユーザのソフトウェアは不正にコピーされたものではないことを通知して(ステップS55)、処理を終了する。また、ディストリビューションIDが正しくなければ、そのユーザのソフトウェアは何らかの形で不正にコピーされたものであることを通知して(ステップS56)、処理を終了する。

【0080】図17は、ソフトウェアに埋め込まれたディストリビューションIDの例を示している。ここでは、例えばWINDOWSのVERSIONINFOリソースを用いて、ディストリビューションIDをファイル内に記録する。図17において、ブロック"040904E4"内に記述された"AAAAAAAA"がディストリビューションIDの埋め込み領域に相当する。

【0081】図18は、このソフトウェアに対応するイ

ンストール用の定義ファイルの例を示している。図18の定義ファイルには、ディストリビューションIDの埋め込み領域を設定したファイルの名称がSOFT.EXEであり、そのアドレス8E80から8文字が埋め込み領域であることが記述されている。

【0082】登録されたソフトウェアの販売時には、ファイルを宅配する前に登録時のオリジナルファイル内のディストリビューションID埋め込み領域を、例えば販売先のユーザのユーザID等書き換える。

【0083】図19は、図17のディストリビューションIDの書き換えを示している。図19において、ファイルSOFT.EXEのアドレス8E80から8E87までに記述された"AAAAAAAA"の8文字が、宅配の前にディストリビューションID"GDF02256"に書き換えられる。

【0084】こうして、販売されたソフトウェアのファイルにそのディストリビューションを識別できる情報が埋め込まれ、必要に応じてファイルからこの情報を読み出すことも可能になる。ディストリビューションIDはホスト計算機11が設定するため、偽りの情報を使用することはできなくなる。また、ディストリビューションIDを埋め込んでいることをユーザに知らせることにより、ソフトウェアの不正コピーを抑制することができる。

【0085】また、ディストリビューションIDにホスト計算機11内だけに持っている情報を加えたり、暗号化技術を組み合わせたりすることにより、ユーザが勝手にディストリビューションIDを書き換えることは非常に困難になる。さらに、ソフトウェア作成者が、作成したソフトウェアの配布ルート等を調べる際にも利用できる。

【0086】

【発明の効果】本発明によれば、オンラインでソフトウェアをインストール販売するシステムにおいて、ソフトウェアの販売履歴を効率的に管理し、ユーザとベンダーの双方にとって有益なサービスが可能となる。

【0087】例えば、配布したソフトウェアが破壊された場合には、販売履歴を確認して、無償の復旧サービスが可能となる。これにより、ユーザはバックアップをとっておく手間が省けるし、ベンダーにとっては不正コピーを監視することができる。また、ユーザの要請に応じて、ソフトウェアがコピーされたものかどうかのチェックを行うこともできる。

【0088】さらに、将来のソフトウェア流通システムにおいて、不正コピーを発見する機構が必要になったときに本発明を適用することもできる。

【図面の簡単な説明】

【図1】本発明の原理図である。

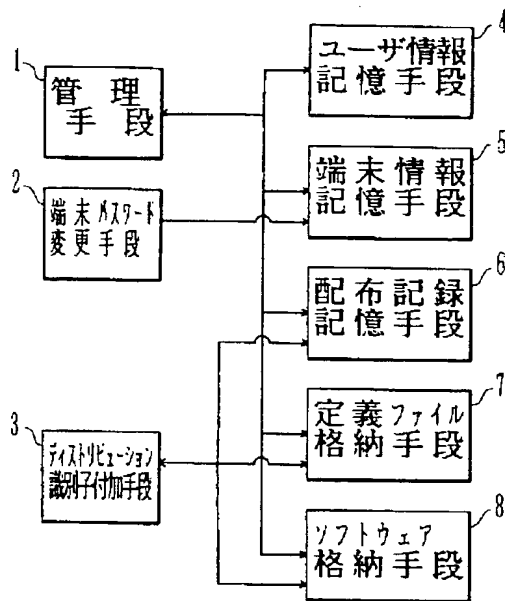
【図2】本発明の実施例のソフトウェア流通システムの構成図である。

17

- 【図3】ユーザ情報を示す図である。
 【図4】マシン情報を示す図である。
 【図5】販売記録を示す図（その1）である。
 【図6】一人のユーザが複数の端末を持つ場合の情報を示す図である。
 【図7】一台の端末を複数のユーザが共有する場合の情報を示す図である。
 【図8】ユーザID登録のフローチャートである。
 【図9】端末ID登録のフローチャートである。
 【図10】販売のフローチャートである。
 【図11】端末パスワードチェックのフローチャートである。
 【図12】端末パスワードのチェック例を示す図である。
 【図13】販売記録を示す図（その2）である。
 【図14】ディストリビューションIDの設定のフローチャートである。
 【図15】ディストリビューションIDの埋め込みのフローチャートである。

【図1】

本発明の原理図



【図3】

ユーザ情報を示す図

UID, PSW, MID, ..., 名前, ...

18.

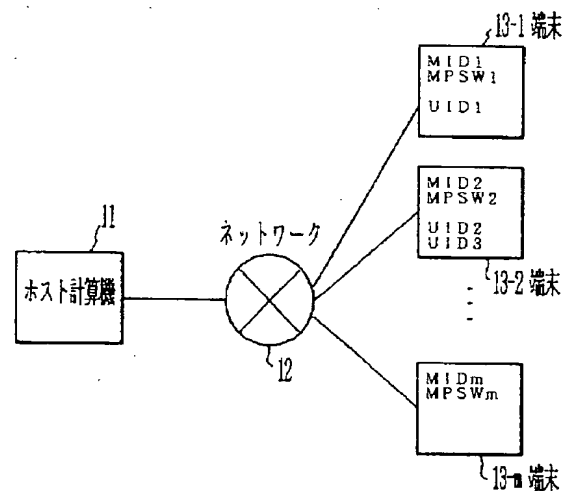
- 【図16】ディストリビューションIDのチェックのフローチャートである。
 【図17】ディストリビューションIDの埋め込み領域の例を示す図である。
 【図18】定義ファイルの例を示す図である。
 【図19】ディストリビューションIDの書き換えを示す図である。

【符号の説明】

- 1 管理手段
 2 端末パスワード変更手段
 3 ディストリビューション識別子付加手段
 4 ユーザ情報記憶手段
 5 端末情報記憶手段
 6 配布記録記憶手段
 7 定義ファイル格納手段
 8 ソフトウェア格納手段
 11 ホスト計算機
 12 ネットワーク
 13-1、13-2、13-m 端末

【図2】

実施例の構成図



【図4】

マシン情報を示す図

MID, MPSW, UID, ..., 機種	販売記録
-------------------------	------

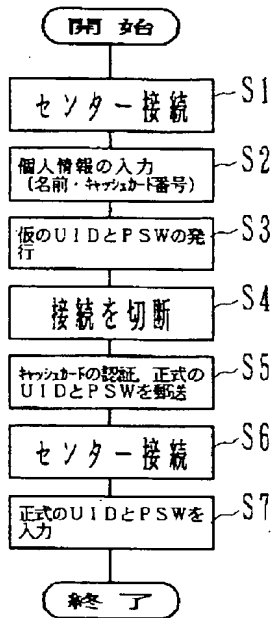
【図5】

販売記録を示す図(その1)

ソフトウェア名	UID	日 時
---------	-----	-----

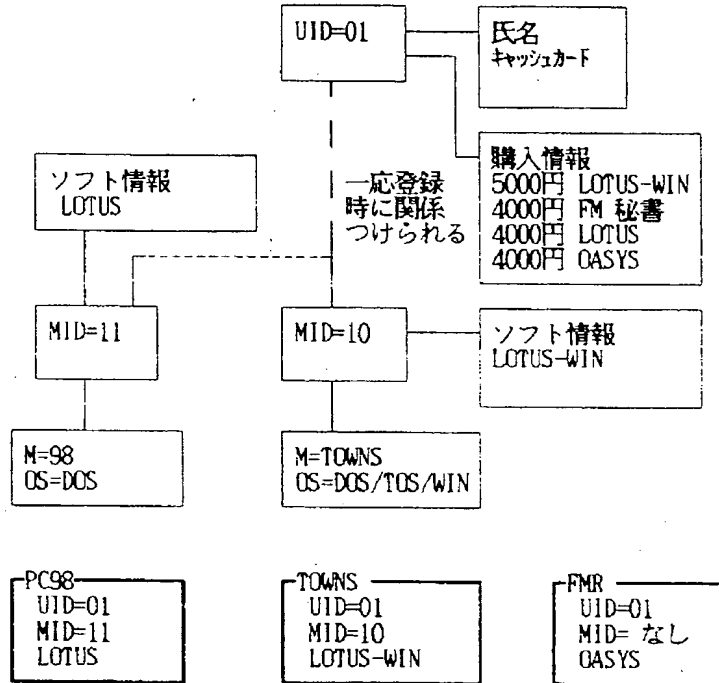
【図8】

ユーザID登録のフローチャート



【図6】

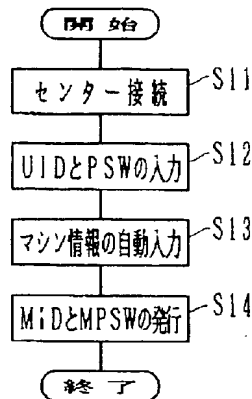
一人のユーザが複数の端末を持つ場合の情報を示す図



【図9】

【図13】

端末ID登録のフローチャート



販売記録を示す図(その2)

ソフトウェア名	UID	日 時	DID
---------	-----	-----	-----

【図17】

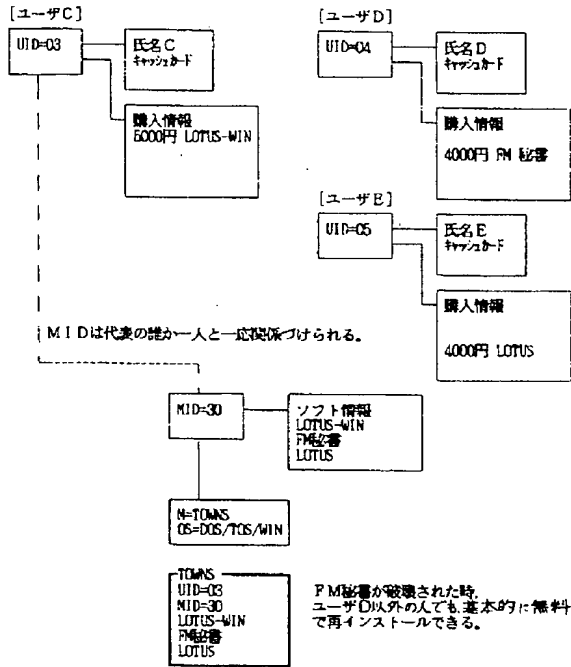
ディストリビューションIDの埋め込み領域
の例を示す図

```

BLOCK "StringFileInfo"
BEGIN
  BLOCK "040904E4"
  BEGIN
    VALUE "Comment", "AAAAAAA"
  ~
  END
END
END
  
```

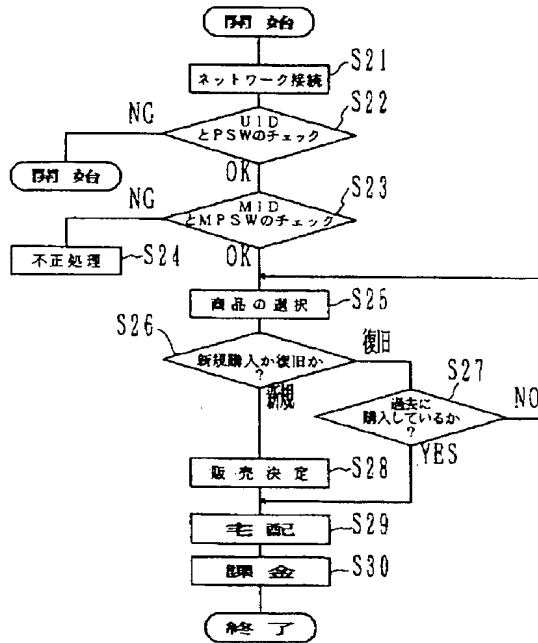
【図 7】

一台の端末を複数のユーザが共有する場合の情報を示す図



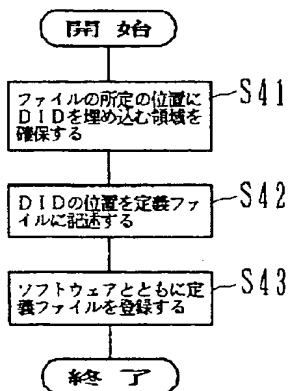
【図 10】

販売のフローチャート



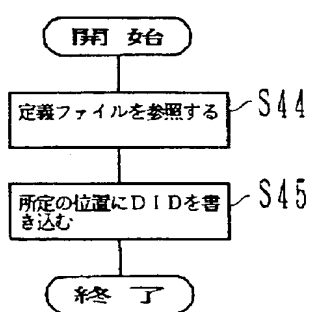
【図 14】

リストバージョンIDの設定のフローチャート



【図 15】

リストバージョンIDの埋め込みのフローチャート



【図 18】

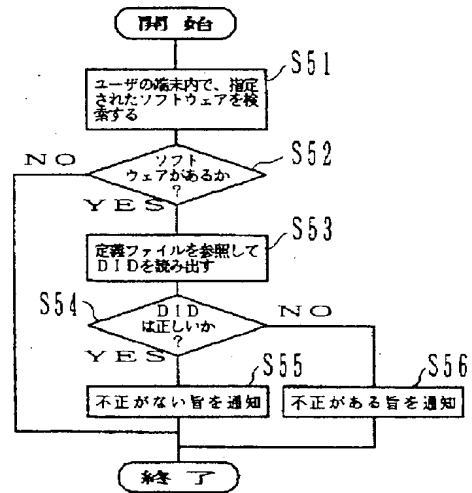
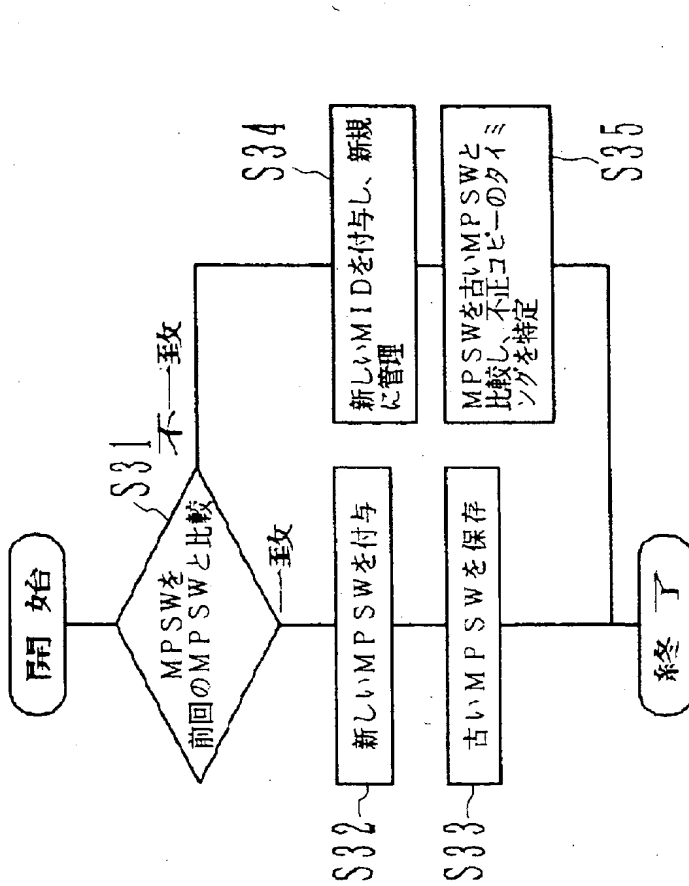
定義ファイルの例を示す図

[MARK]
FILE=SOFT.EXE
index=8E80
NUM=8

【図11】

【図16】

端末パスワードチェックのフローチャート ディストリビューションIDのチェックのフローチャート



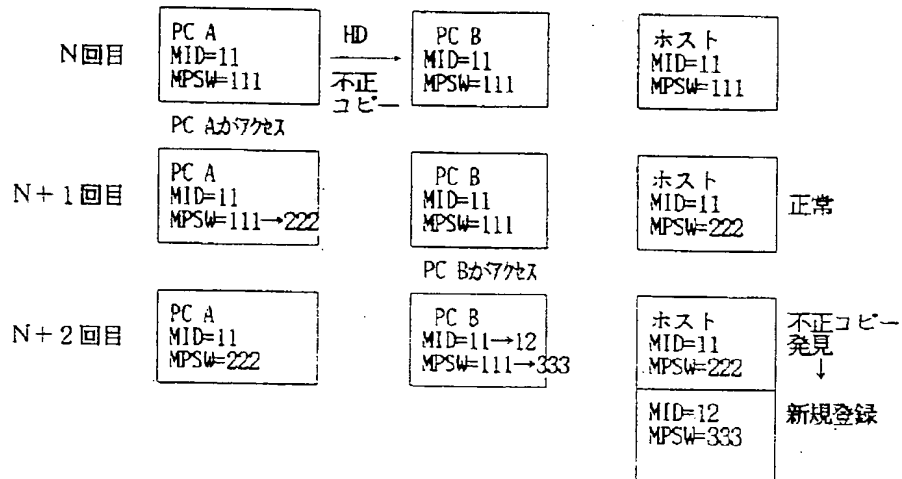
【図19】

ディストリビューションIDの書き換えを示す図

8E80	8E81	8E82	8E83	8E84	8E85	8E86	8E87
A	A	A	A	A	A	A	A
↓							
8E80	8E81	8E82	8E83	8E84	8E85	8E86	8E87
G	D	F	0	2	2	5	6

【図12】

端末パスワードのチェック例を示す図



フロントページの続き

(51)Int. Cl. 6
G 0 6 F 17/60

識別記号 庁内整理番号

F I

技術表示箇所

(72)発明者 沖 宏志
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者 鎌田 紳二
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者 原 孝
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(72)発明者 山崎 利哉
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内